How the Pandemic Affected IT Supply Chain

A new report lists the biggest weaknesses in the ICT supply chain and what private and federal IT leaders can do to eliminate them.

Kate Macri
Tue, 11/24/2020 - 15:30

The COVID-19 pandemic exposed vulnerabilities in information and communication technology (ICT) supply chains once considered industry best practices. The divergent needs of federal and private sector supply chains suggest that federal agencies, in particular, should revamp their approach to supply chain management and security in response to the pandemic’s effect on the global IT supply chain.
In a new report, the Cybersecurity and Infrastructure Security Agency (CISA) highlighted lean inventory management models and a lack of supply chain visibility behind Tier 1 suppliers, and an overreliance on single-source suppliers as key drivers of disruption to ICT supply chains during the pandemic.

CISA advises federal agencies and ICT companies to create broader maps of their ICT supply chains and move away from the “just-in-time” inventory management style of private industry, a trend started by e-commerce companies to beat out big-box retailers and now a mainstay of supply chain management.

“Increased competition and often-compressed profit margins have driven supply chain managers to emphasize cost reduction, just-in-time deliverables and days of supply inventory management,” CISA said in the report. “Companies may also continue to push for vendor-managed inventory, a scenario under which among other things, a supplier is paid a fee to hold extra equipment on hand in their warehouses. Firms look to this practice as Wall Street often punishes those publicly traded firms that hold too much inventory on their books.”

In other words, the pursuit of maximum efficiency for the sake of wider profit margins crippled ICT supply chains when COVID-19 swept the globe.

This inventory management practice harmed ICT companies and their federal customers when the pandemic hit because warehouses ran out of inventory, leaving orders unfulfilled. Without an inventory “cushion,” suppliers for federal and industry customers simply could not keep up with demand.

“During the pandemic, under this practice, inventories ran short due to fulfillment delays,” CISA said in the report.

The other two main drivers of supply chain disruptions this year — visibility beyond Tier 1 suppliers and overreliance on single-source suppliers -- are interconnected. IT companies and federal agencies need to create broader, clearer maps of their entire supply chain, including visibility into their Tier 2 and Tier 3 suppliers’ inventory management systems and raw materials.
CISA cited a 2019 BCI Supply Chain Resiliency report, which “showed that most supply chain incidents are caused by disruptions in a company’s tier 2 and tier 3 supplier base,” further emphasizing the need for exhaustive visibility.

The Cyberspace Solarium Commission also elaborated on the risk of relying on single-source suppliers in its latest report on ICT supply chain security. For example, the U.S. relies heavily on China and countries susceptible to Chinese influence (like Taiwan) for raw materials for ICT products and various stages of ICT production.

Because the pandemic originated in China and affected Chinese suppliers and manufacturers first, the IT supply chain took an especially critical hit this year.

“Many suppliers [in China] ‘went dark’ for several weeks at the onset of the pandemic, as factories were shut down and suppliers were also simply overwhelmed,” CISA said in its November report.

To combat these risks, CISA suggests companies and federal agencies focus on mapping their supply chains, diversifying their “supplier network and regional footprint,” and allowing suppliers to hold a more substantial buffer of inventory.

“The United States and other advanced industrial economies have created a highly efficient and effective manufacturing-and-delivery system that provides them with a wide variety of products at relatively low costs,” CISA said. “But integral to that system are the dependencies and expectations that the pandemic has called into question. Going forward, U.S. firms in the ICT sector should continue to diversify their supply chains and inventory practices, albeit at a pace that takes into account economic realities.”

View printer friendly version
Cybersecurity and Infrastructure Security Agency
CISA
ICT supply chain
IT supply chain
coronavirus
pandemic
Standard